WHO'S THAT KNOCKING AT MY COMPUTER?

BY MARY SIERO

Data breaches have become so common that they don't make the news much anymore. However, they are still happening in alarming numbers. Released in April, the Verizon 2011 Data Breach Investigation Report stated that while total data record loss is down, the number of incidents is higher and the method of attack is much more diverse than it has been in the past.

In the past few years hospitality has become an increasingly inviting target due to the highly desirable information generally found in these systems. Coupled with the fact that it can take a long time to trace fraudulent transactions back to their origin and that many companies are putting off system upgrades and implementation of security software during the downturned economy, and you have what looks like a jackpot for hackers. Verizon confirmed in this year's report that hospitality is still a favored target (40 percent of all breaches it investigated) and speculated:

"Criminals may be making a classic risk vs. reward decision and opting to 'play it safe' in light of recent arrests and prosecutions following large scale intrusions into financial services firms. Numerous smaller strikes on hotels, restaurants and retailers represent a lower-risk alternative, and cybercriminals may be taking greater advantage of that option."[1]

A quick search pulls up breaches in the first quarter of this 2011 for Ambassador Hotel Group-Korea (3/4/11)[2], Se San Diego Hotel (3/9/11)[3], Nations Giant Hamburgers (3/16/11)[4], Shell Vacations Hospitality (1/27/11)[5] and Epsilon who managed messaging for several hospitality clients, just to name a few.

If you take a quick poll among your friends, you will find that most people assume the majority of hackers are people working alone to steal your identity and/or your financial information; teenagers or people who were otherwise misdirected in their youth. The truth is that most hackers are part of organized crime rings centered in Eastern Europe; a cyber bratva (slang for Russian brotherhood) of sorts.

The cyber bratva could rival some of our most successful legitimate companies. In fact, an entire industry has been built up around these organized crime rings.

There are educational websites for hacker wannabes. The legitimate ones are easy to find and include ethics in their education. These are the people you want to hire to see how impenetrable your systems are because they are hackers with a conscience. If they think that something they might do would harm your network or data, they will stop and talk to you about it. There are also underground sites that you need to be invited to or referred to from others. These are the people who aren't looking to be employed by you.

Hackers have shopping sites where they can go to buy the tools they need to break into your systems. They can almost order from a menu so that the tool they buy will exploit the specific technologies you have implemented. In addition there are electronic bulletin boards, books, chats and other forums where the would be thieves can round out their education, and most of it is completely legal. Sure they have disclaimers regarding the use of these products, but do you think bad guys care to read the fine print?

Like any business, the cyber bratva consists of individuals who specialize in various areas of their enterprise. They all require different skill sets and educations, and their performance reviews are evident in their financial successes and abilities to elude detection or arrest.

Some of the jobs are back of the house, such as the coders or programmers who write the malware or scanning systems to break into your network, the technicians who maintain their IT infrastructure, and the hackers who use the tools created by the coders to actually break into your network and harvest your data. Others are more in the marketing or sales area: the fraudsters who create and use phishing, scam or other social engineering tactics and the distributors who advertise for and sell or trade stolen data so that it can be converted to cash by someone else. There are those in finance who create drop accounts, provide names and accounts to others for a fee and the money mules that complete the wire transfers between bank accounts. Lastly, these groups have presidents and CEOs who determine whether to reinvest their profits in additional assets to expand their criminal enterprise, identify target industries for exploitation, and ensure that the business remains profitable by keeping abreast of the legal landscape in the countries they operate in so that they can avoid detection.

However, despite that their business model is at least as good as yours, there are a few things you can do to be less attractive to them and keep ahead of them.

First, keep your systems current. It can be tempting to put off a system upgrade to save some money until the economy gets a little better. Before you do that, find out whether the upgrade plugs any security holes or exit points in your software or enables you to use third-party software that is more secure. If it does, lower your risk by upgrading your system. Second, ensure your staff receives regular security awareness training. Social engineering will overcome security software every time; don't let it do so by making sure your employees are educated and understand their roles in keeping your company secure. Lastly, conduct regular security or vulnerability assessments and rotate the vendors who perform them ever two to three years to ensure you are getting fresh perspectives. Consider any recommendations and implement them based on your tolerance for risk as an organization.

MARY SIERO, CISSP, CRISC *is the principal at Innovative IT in Las Vegas, www.innovativeitlv.com.*

(Footnotes) [1] 2011 Verizon Data Breach Investigation Report
[2]http://tinyurl.com/4vqjkhv
[3]http://datalossdb.org/incidents/3419
[4]http://www.ktvu.com/news/27219035/detail.html
[5]http://tinyurl.com/3ztlc6t